EXHIBIT 25

4-May-95

SW Functional Spec Rev 1.0
Author: Bill Westfield
Project Mgr: Andy Valencia

Radius Protocol Support

Abstract

RADIUS is an access server authentication and accounting protocol developed by Livingston, Inc. It has gained support amoung a wide customer base, and is expected to be run through the IETF for standardization as a NAS authentication protocol. RADIUS is currently defined in draft documents on ftp.livingston.com:pub/radius/draft-ietf-radius-radius-03.txt. The cisco implementation will be based on this version of the draft, and attempts will be made to keep up with any newer drafts issued.

Approvals

Modification History

Rev	Date	Originator	Comment
1.0	950504	Bill Westfield	Initial Release

1.0 Definitions

Authentication - The means by which you IDENTIFY your self to the cisco.

Authorization - The means by which the cisco determins what actions you mat perform.

Accounting - the means by which the cisco tracks what you have done.

AAA cisco's security paradigm (Authentication, Authorization, Accounting) In theory, AAA is protocol independant.

TACACS+ cisco's network protocol for implementing AAA. TACACS+ is tcp based.

NAS - Network Access Server. The cisco Access Server, or other cisco hardware, that is acting as the client fo the authentication protocol.

2.0 Problem Definition

Some large customers have settled on RADIUS as their standard for network based authentication, and request that we implement it. Radius does not appear to have any features not supported by Tacacs+, and lacks a few nicities that would allow it to map cleanly onto AAA, so it should be moderately easy to add support for.

The most important consideration are to support per-user service definition and network profiles. Eg, when user "billw" logs in, RADIUS must be able to specify that ppp using ip address x.y.z.a and access-list N should be started.

3.0 Design Considerations.

Radius combines the Authentication and Authorization functions, so the NAS will have to "remember" authorization information from the authentication response, and supply that later on when requested by authorization. The NAS must be configured for the appropriate authorization or it will ignore that data from the authentication packet.

RADIUS is UDP based. A single process should be responsible for multiplexing and demultiplexing multiple authentication "streams" between the NAS and the Radius Server. While we're at it, do this for tacacs+ as well.

RADIUS should be a separate subsystem, so that it can be omitted from images (eg rxboot) where it is inappropriate.

4.0 Memory and Performance Impact.

The RADIUS code should add less than 30k to the image size, use negligible memory other than packets queued awaiting answers, and have negligible performance impact in general and none in any critical paths.

5.0 End User Interface.

No new end user interface. (Note that radius is capable of supplying login dialog to the user during authentication, and can provide a different user interface there.)

6.0 Configuration and Restrictions.

It should be possible to specify "radius" anywhere in config files where "tacacs+" is currently usable. Authentication and authorization lists that allow multiple protocols to be specified should allow both tacacs+ and Radius, in either order.

aaa authentication <feature> <listname> RADIUS

aaa authorization <feature> RADIUS

aaa accounting <feature> <when> RADIUS

In addition, a set of top level "radius-server" commands analagous to the "tacacs-server" commands will be added:

radius-server host <list> Server host to use.

radius-server key <string> Key for encryption.

radius-server retransmit <n>	Max number of retransmission attempts.
radius-server timeout <n>	Time between retransmisions.
radius-server directed-request	Allow user to specify "@server"

radius-server refuse-unimplimented

This is new. For features that are implemented in the cisco NAS, but are not supported by the current version of the radius protocol, refuse to let the user use those features. The default is "no radius refuse", which allows the feature to be used without attempting a radius transaction.

radius-server shell-doauth (???)

This command is an attempt to use radius authentication calls to do authorization. If the Server grants the user "shell" access during the initial authentication, the NAS will normally allow any shell commands that are not explicitly disallowed by any additional authorization info from that original authentication. If "radius shell-doauth" is configured, the NAS will issue additional authentication requests for new commands, with no password included (this is one suggested method of doing authorization within the current radius protocol.) Few servers are expected to support this.

7.0 Testing Considerations.

Should be tested against existing radius servers from UWisc/etc.

8.0 Reference Documents.

AAA specification. TACACS+ Specification. Radius draft specification.